PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-105057

(43)Date of publication of application : 24.04.1998

(51)Int.Cl. G09C 1/00
G06F 13/00

(21)Application number : 08-253600

(22)Date of filing : 25.09.1996

(71)Applicant : HITACHI SOFTWARE ENG CO LTD

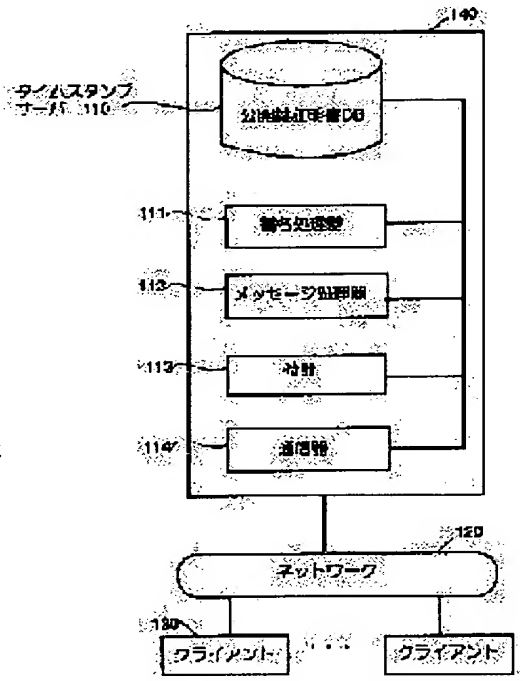
(72)Inventor : SAMEJIMA YOSHIKI

(54) TIME STAMP SERVER SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To make it possible to generate and use information which can be used as an evidence proving that computer data already existed at a time point in the past, to protect information against being leaked by a third party by making a writer/sender/addressee, and data of a message confidential, and to realize a register function and anthentification service to keep an evidence of transmission and receipt of data and message.

SOLUTION: This time stamp server system is constituted to include an identifier of an algorithm used to generate a message digest of data and additionally a parameter in subject data of a digital signature in a demand message and a reply message. Further, the system is constituted to include identification information of data, message digest of data, creator of data, and sender/ addressee of an electronic message in a demand message and a reply message together with a cryptograph, a message digest of a decoding key, a public corresponding to a decoding key.



LEGAL STATUS

[Date of request for examination] 30.03.1999

[Date of sending the examiner's decision of rejection] 29.03.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] It is the time stump server system characterized by connecting two or more clients, including a parameter in the identifier and addition target of an algorithm which used it for a time stump server generating the message digest of data to data transmission of a client at the object data of the digital signature in a demand message and an answerback message in the network system which consists of the time stump server which offers specific service, and answering a client.
[Claim 2] Data transmission of a client is received in a time stump server system according to claim 1. In the reply message by the time stump server, the message digest of data, The algorithm identifier used for generating a message digest, In any one of the parameters at the time of using it for generating a message digest, or each combination, Or the above-mentioned information which carried out the code and the message digest of the key which decodes a code, The identifier of the algorithm used for message digest generation of a key, The identifier of the parameter used for message digest generation of a key, and the algorithm used for the code, Any one or each combination of the parameter used for the code, Or the message digest of the data which carried out the code, and the key which decodes a code, The identifier of the algorithm used for message digest generation of a key, The identifier of the parameter used for message digest generation of a key, and the algorithm used for the code, With any one of the parameters used for the code, or each combination, Or the data which enciphered the key which decodes the above-mentioned code using the public key, said public key, and the algorithm identifier of a public-key-encryption algorithm, The parameter of a public-key-encryption algorithm, and the identifier of the algorithm used for the code, Or a demand message is received from a client including either of each combination. any one of the parameters used for the code -- Time information and the above-mentioned information included in the demand message from the client, The identifier of the algorithm used for digital signature generation including the digital signature to time information and the information included in the demand message from the client, Either of the parameters additionally used for digital signature generation, or the time stump server system characterized by transmitting combination as an answerback message.
[Claim 3] The time stump server system characterized by transmitting an answerback message to a client using the digital signature generation time of day in the answerback message sent to any one and the client of the time of day which received the demand message from a client as time information, the digital signature generation time of day in the answerback message sent to a client, and the time of day which received the demand message from a client in a time stump server system according to claim 1 or 2.
[Claim 4] The attached information on the data which came the origin of a message digest into the demand message from a client in the time stump server system according to claim 1 or 2, In any one of the message digest of attached information, and the enciphered attached information, or each combination, The message digest of the key which decodes a code, and the identifier of the algorithm used for message digest generation of a key, The identifier of the parameter used for message digest generation of a key, and the algorithm used for the code, In any one of the parameters used for the code, or each combination, The message digest of the attached information which carried out the code,

and the message digest of the key which decodes a code, The identifier of the algorithm used for message digest generation of a key, In any one of the parameter used for message digest generation of a key, and the parameters used for the code at the identifier and addition target of the algorithm used for the code Or the time stump server system characterized by including and transmitting to an outgoing message as object information on the digital signature in an answerback message including each combination.

[Claim 5] The time stump server system characterized by performing the effectiveness check of the public key certificate with which a server program contains the digital signature to the public key of public key encryption, the information containing said public key owner's identifier, and said information in a time stump server system according to claim 1 or 2.

[Claim 6] The time stump server system characterized by using portable data storage media, such as a floppy disk, and a magnetic tape, an optical disk, and carrying out the exchange of a server, the demand message between clients, and an answerback message in one of time stump servers according to claim 1 to 5.

[Claim 7] The time stump server system characterized by proving that the data which became the origin of the message digest in a demand message existed before from the time information in an answerback message by verifying the digital signature contained in answerback information from a time stump server in one of time stump server systems according to claim 1 to 6.

[Claim 8] The time stump server system characterized by using public key encryption or a secret key cryptosystem as a digital signature of an answerback message in one of time stump server systems according to claim 1 to 7.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the informational generation and the use which can be used as a proof to which computer data already exist and prove things, when computer data, such as a file, an electronic message, and a document, are applied to the technique in connection with the certification of having existed in a certain time, especially have the past.

[0002]

[Description of the Prior Art] As a fundamental concept of time stump service, it is [: There is Non-repudiation.] ISO/IEC DIS 10181-4.2 Information technology. -- Open SystemsInterconnect ion -- Security frameworks in Open Systems -- Part 4

[0003] The message digest of data or data was contained in the demand message to the time stump server shown in this fundamental concept.

[0004]

[Problem(s) to be Solved by the Invention] However, when using a message digest in the above-mentioned fundamental concept, neither the information on the algorithm used for generating a message digest nor the parameter information in the case of generation is included. For this reason, in case the answerback message which is the proof of data existence is verified, although the message digest was generated how, it does not understand.

[0005] Moreover, it was possible to have given false evidence as having existed, when there were data which used it on the occasion of proof of a different algorithm from the algorithm which originally generated the message digest, forged the message digest, and did not exist in fact.

[0006] Moreover, data might be specified from the message digest and a generation request of the time stump of data to make it secret was not completed in a time stump server at a time stump generate time.

[0007] Moreover, in the above-mentioned fundamental concept, it had suggested that an addresser and recipient information when the implementer of data and data are electronic messages were included in a demand message. For this reason, there was a problem that a data origination person, and the addresser/addressee of an electronic message will be known by the management person of a time stump server or a time stump server.

[0008] When the purpose of this invention has the past, it is for the information which can be used as a proof to which computer data already exist and prove things to generate and use it, secrecy-izes the implementer / addresser / addressee of a message, and data further, and is to prevent leakage of the information by the 3rd person. For example, on the occasion of CALS or electronic banking, the registered mail function and authentication service which only leave the proof of transmission and reception of data, not only the code and authentication of a cut-form and an electronic message but data, or a message are set to one of the purposes of this invention.

[0009]

[Means for Solving the Problem] It is made for a parameter to be included in the identifier and addition target of an algorithm which used it for generating the message digest of data in a demand message, and was made to include a parameter in an identifier or an addition target for [in the answerback message of a server] a signature in this invention.

[0010] Furthermore, the message digest of a code and a decode key also included the message digest of data or data in the demand message or the answerback message, the code of the decode key was carried out with the public key, and the code data and the public key of a result were included.

[0011] Moreover, the message digest of a code and a decode key is also a demand message and answerback message ****** about the identification information of the implementer of data, the addresser of an electronic message, or an addressee.

[0012]

[Embodiment of the Invention] Hereafter, the gestalt of 1 operation of this invention is explained to a detail using a drawing.

[0013] Drawing 1 is drawing showing the whole this invention configuration.

[0014] The time stump service system 140 consists of two or more clients 130 using the time stump server 110, a network 120, and a time stump server. The time stump server 110 is constituted by the public key certificate DB111, the digital signature treater 112, the message-processing machine 113, a clock 114, and the communications apparatus 115.

[0015] To the demand message from a client 130, the time stump server 110 adds time information, and returns the answerback message which gave the digital signature.

[0016] The public key certificate DB111 is a database which stores the information on the public key certificate represented by international standards X.509, and returns the answerback discarded [the owner effect, an invalid, and] to the certification letter voice inquiry from the message-processing machine 113. In the case of an invalid, the time and the reason which became an invalid can also be returned.

[0017] The signature generation machine 112 generates the digital signature of an answerback message to the request from the message-processing machine 113. It is common to generation of a digital signature to use the technique of a message digest which is in international standards X.509, and public key encryption.

[0018] Although a message digest is the result of changing the digital data of arbitration length into the data of fixed length, there are following various troubles.

[0019] It is difficult in computational complexity to discover different data with the same message digest, and it difficult to guess the original data from a message digest. Furthermore, it has the property in which it is difficult to constitute the data which become a certain message digest.

[0020] Moreover, the public key encryption used here is a code in which the key used for a code differs from the key used for decode, and unless it does a code/decode of with a corresponding cryptographic key and a corresponding decode key, it cannot decode correctly. Moreover, a digital signature is combining these two techniques, and is inspecting the bona fides of the alteration detection [of data], and creation origin of data.

[0021] The message-processing machine 113 is performed using other components for the analysis of a demand message and the generation of an answerback message which the client has led. The clock 114 holds current time and returns current time to the demand from the message-processing machine 113.

[0022] In addition, amendment of time of day is based on the clock of a time stump server in this invention, and each client is based on this time of day. The average of the time of day of all machines may be used.

[0023] The communications apparatus 115 is processing the communication link of the message exchanged between the time stump server 110 and a client 130 through a network 120. A network 120 connects a client 130 with the time stump server 110, and relays the demand message and answerback message which are exchanged.

[0024] A client 130 transmits requested data including the message digest of data, and other information to the time stump server 110, and receives the answerback (message time stump certificate) which the digital signature attached. When a server receives a demand message, an answerback message is kept so that it can use later as a proof which shows that the data which became the origin of a message digest existed.

[0025] Some of information which is mentioned to Table 1 is included in the demand message.

[0026]

[Table 1]

(1)存在証明が必要なデータのメッセージダイジェスト (2)(1)に付加的につけられるメッセージダイジェストを生成するのに使用したメッセージアルゴリズムの識別子 (3)(1)に付加的につけられるメッセージダイジェストを生成するのに使用したアルゴリズムのパラメータ
(4)上記(1)(2)(3)メッセージダイジェストを生成するのに使用したアルゴリズムのパラメータ
(5)作成に使用した編集プログラムのファイルフォーマット識別情報、印刷用記述言語識別情報などのデータ形式を示す情報 (6)文書作成者 (7)文書の作成日時 (8)文書のタイトル (9)文書識別番号 (10)電子メッセージの発信者 (11)電子メッセージの受信者 (12)電子メッセージの識別子

[0027] Drawing 2 shows a demand message when a code is carried out also to the message digest of

data, and the attached information on data.
[0028] Data 201 are the message digest of data, and the result of enciphering a parameter on the generation algorithm identifier and addition target of a message digest additionally. Data 202 are the message digest of the key which decodes an item 201. "DES-CBC" of an item 203 is the identifier of the algorithm which used the message digest of data etc. for carrying out a code. The data of 204 are the parameter which used the message digest of data for carrying out a code.
[0029] Drawing 3 is an example of the answerback message from a server to a client, and shows the answerback to the requested data of drawing 2 .
[0030] "19960713142347" of an item 301 shows that the generation time of the digital signature 303 in an answerback message is "14:23 47 seconds on July 13, 1996." An item 302 is data for a signature. The data of an item 303 are the signature of the server to an item 301 and an item 302. "RSAEncryptionWithMD2" of an item 304 shows a signature generation algorithm. It is shown that "NULL" of an item 305 did not use a parameter for the signature generate time.
[0031] Drawing 4 is an example of the demand message from a client to a server.
[0032] An item 401 is the message digest of data. "MD5" of an item 402 is the identifier of the algorithm used when generating the message digest of data. "NULL" of an item 403 shows having not used a parameter, when generating the message digest of data. An item 404 to the item 408 shown below is an example of the additional information of data, and the effectiveness confirmed information of a public key certificate.
[0033] "Editer" of an item 404 is the formal information on the document of data. "The patent detail of a time stump" of an item 405 is the document title of data. "** ** O ****" of an item 406 is the document preparation person name of data. "3459" of an item 407 is a serial number which is the information for identifying a public key certificate. "19960622171129" of an item 408 shows ****** whose time which carries out the effectiveness check of a public key certificate is "17:11 29 seconds on June 22, 1996."
[0034] Especially drawing 5 shows the answerback message which included invalid information in the information on the effectiveness check of a public key certificate, and this case.
[0035] It is shown that "19960713142345" of an item 501 received the demand message from a client at "14:23 45 seconds on July 13, 1996." The data for a signature of an item 502 were contained in the demand message, and are equivalent to drawing 4 in this case. An item 503 shows that the public key certificate is an invalid. 504 shows the reason which became an invalid. It is shown that the individual key corresponding to a public key suited the theft of 19960621125634 ["19960621125634"] of an item 505 at "12:56 34 seconds on June 21, 1996." "3459" of an item 506 is a serial number for identifying the public key certificate which became an invalid. An item 507 is the signature of the server to the item 506 from an item 501.
[0036] Hereafter, actuation of the time stump server 110 is explained to a detail according to drawing 6 .
[0037] A communications apparatus 115 receives the demand message (drawing 2) sent through a network 120 from the client 130, and passes it to the message-processing machine 130 (step 601).
[0038] The message-processing machine 113 takes out the data 201, 202, 203, and 204 for a signature from a demand message, and follows the format of the information defined beforehand, or inspects how (step 602). The message-processing machine 113 accesses a clock 114, and obtains current time (step 603).
[0039] The message-processing machine 113 doubles time information with the data 201, 202, 203, 204, and 302 for a signature, and sends it to the signature treater 112 (step 604). The signature treater 112 generates a digital signature from the data for a signature, and time information, and returns it to the message-processing machine 113 (step 605).
[0040] The message-processing machine 113 constitutes an answerback message (drawing 3) from the data 302 for a signature, time information 301, a digital signature 303, a signature algorithm 304, and a parameter 305, and passes it to a communications apparatus 115 (step 606). A communications

apparatus 115 sends an answerback message to a client 130 through a network 120 (step 607).
[0041] Next, the time stump service processing combined with public key certificate check service using drawing 7 is explained.
[0042] A communications apparatus 115 receives the demand message sent through a network 120 from the client 130, and passes it to the message-processing machine 130 (step 701). The message-processing machine 113 accesses a clock 114, and obtains current time (step 702).
[0043] The information for identifying the following public key certificates is included in a demand message [other than the example of said drawing 4]. They are the owner of the identifier of published certificate authority Certification Authority, a serial number, a public key public key, and the individual key private key, and the time which checks effectiveness.
[0044] By the demand message of drawing 4 , a serial number is contained in an item 407 and effectiveness check time is included in the item 408. The message-processing machine 113 takes out the above-mentioned information, and it inspects whether the format of the information defined beforehand is followed (step 703).
[0045] The message-processing machine 113 asks the effectiveness of delivery and a certificate to the public key certificate DB111 for the identification information (item 407) of the above-mentioned public key certificate, and the time information (item 408) which checks effectiveness (step 704).
[0046] The public key certificate DB111 is searched based on certificate identification information, the effectiveness of the public key certificate in the time information time which checks effectiveness is checked, and a result is returned to the message-processing machine 113 (step 705). It is [of the owner effect, an invalid, and an invalid] reasonable as a result of a check.
[0047] The message-processing machine 113 doubles time information with the data 401, 402, 403, 404, 405, 406, 407, 409, 408, and 502 for a signature, and a certificate effectiveness check result, and sends it to the signature treater 112 (step 706).
[0048] The signature treater 112 generates a digital signature from the data for a signature, a certificate effectiveness check result, and time information, and returns it to the message-processing machine 113 (step 707). The message-processing machine 113 constitutes the answerback message (drawing 5) which consists of the invalid 503 of the data 502 for a signature, time information 501, and a certificate effectiveness check result, the reason 504 for an invalid, the invalid time 505, a certificate identification number 506, and a digital signature 507, and passes it to a communications apparatus 115 (step 708). A communications apparatus 115 sends an answerback message to a client 130 through a network 120 (step 709).
[0049] Next, the authentication service using an answerback message, i.e., a time stump certificate, is explained using drawing 8 .
[0050] If the providers of service who prove / guarantee that reached with the time stump service provider which manages a time stump server especially, and document data existed in a certain time of day using the time stump certificate are a country and a municipal corporation, it will become possible to adopt as a proof of a trial in the future.
[0051] A notary receives the key of decode from a certification candidate, when the code of the message digest of the data of a time stump certificate is carried out further, a time stump certificate, object data, and (step 801).
[0052] The digital signature of a time stump certificate checks whether it is the right. When the public key certificate is being especially used as a signature, a signature is checked using the public key of a time stump server (step 802). When the code of the message digest of the data contained in a time stump certificate is carried out, it checks that the message digest of the received decode key and the message digest of the decode key in a time stump certificate are in agreement (step 803).
[0053] When the code of the message digest of the data contained in a time stump certificate is carried out, it decodes using a decode key and the message digest of data is obtained (step 804).
[0054] The message digest of the received data is calculated and it checks that it is in agreement with

the message digest of the data obtained from the time stump certificate. If in agreement, it will guarantee that the data concerned existed before the time of day contained in the Daim stamp certificate (step 805).

[0055] The gestalt of operation of this invention at the time of using public key encryption using drawing 9 and 10 is explained.

[0056] An item 901 is data which become candidates for a signature, such as a document which carried out the code. A private key symmetry key code is usually used for a code. An item 902 carries out the code of the key which decodes the data of an item 901. Public key encryption is used for a code. An item 903 is the public key used for the code of an item 902. An item 904 is the identifier of the algorithm of public key encryption. An item 905 is the identifier of the algorithm which carried out the code of the data of an item 901. The answerback message of the time stump server of the demand message of drawing 9 is indicated by drawing 3 , and since it is the same as that of drawing 6 , processing is omitted. The data 302 for a signature of an answerback message correspond to a demand message (drawing 9 R> 9).

[0057] Next, the authentication service at the time of using a public key using drawing 10 is explained.

[0058] A notary receives the individual key corresponding to a time stump certificate, i.e., answerback message drawing 3 and the public key to a demand message of drawing 9 , from a certification candidate (step 1001).

[0059] Next, the digital signature of a time stump certificate checks whether it is the right (step 1002). The approach of a check is the same as that of the above-mentioned step 802. Next, it checks whether the individual key thought to be the public key contained in a time stump certificate corresponds (step 1003). The public key is the same as the item 903 of the demand message of drawing 9 corresponding to the item 302 of a time stump (drawing 3), i.e., an answerback message.

[0060] A data decode key is obtained by decoding the decode key (it being the same as 902 of the demand message of drawing 9) which carried out the code using the individual key. The algorithm used for decode is a public-key-encryption algorithm corresponding to the identifier which hits 904. (Code data and an item 901) are decoded with the obtained decode key, and the data for a signature are obtained (step 1005). The algorithm used for decode is an algorithm corresponding to the identifier which suited the demand message 905.

[0061] It can prove that data existed by this before the time of day contained in a time stump certificate.

[0062]

[Effect of the Invention] the identifier of the algorithm used when creating a message digest from the data which need the proof of existence as mentioned above at this invention -- additional -- a parameter -- demand message ****** -- making it like, the time stump server is carrying out the digital signature based on such information. For this reason, it is turned out using what kind of algorithm to have generated the message digest, and how since it is contained in the answerback message which is proof, proof should be verified. Moreover, with the approach which actually generated the message digest of data, since it can prevent creating a message digest by the option at the time of verification, perjury can be prevented.

[0063] Moreover, it becomes possible to request a server also to data to make it secret at a time stump server at a time stump generate time by using as the data for a signature the message digest of the data which carried out the code instead of the message digest of data. Moreover, also when the code of the data is carried out as another means and the code of the decode key is carried out with a public key including the message digest of a decode key, the same effectiveness can obtain.

[0064] Moreover, since the code of the identification information of the implementer of data, the addresser of an electronic message, or an addressee is carried out and it was made to include a demand message and an answerback message, it becomes possible to get the signature of a time stump server to the additional information of data including a data origination person, or the addresser and addressee

of an electronic message, without being known by the management person of a time stump server or a time stump server.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] They are the whole time stump service configuration and the internal configuration Fig. of a time stump server.
[Drawing 2] It is a demand message block diagram containing a message digest.
[Drawing 3] It is an answerback message block diagram to the demand message of drawing 2 .
[Drawing 4] It is a demand message block diagram containing the message digest which carried out the code.
[Drawing 5] It is an answerback message block diagram to the demand message of drawing 4 .
[Drawing 6] It is the flow chart which shows basic actuation of a time stump server.
[Drawing 7] It is the flow chart which shows actuation of the time stump server at the time of combining with effectiveness check service of a public key certificate.
[Drawing 8] It is the flow chart which shows actuation of the testifier notary who checks existence of the data using a time stump certificate.
[Drawing 9] It is a demand message block diagram at the time of using a public key by claim 1.
[Drawing 10] It is the flow chart which shows actuation of the testifier notary who checks existence of the data at the time of using a public key by claim 1.
[Description of Notations]
110 -- A time stump server, 111 -- The public key certificate DB, 112 -- Digital signature treater, 113 -- Demand / answerback message-processing machine, 114 -- A clock, 115 -- Communications apparatus, 120 -- A network, 130 -- A client, 140 -- Time stump service system, 201 -- The message digest of the data for a time stump, and the result of having carried out the code of an algorithm and the parameter additionally, The message digest of the key which decodes 202--201, the identifier of the algorithm used for the code of 203--201, The parameter, 301 which were used for the code of 204--201 -- Generation time of a digital signature, 302 -- The data for certification, 303 -- The signature of a server, 304 -- Signature generation algorithm identifier, 305 -- A signature generation parameter, 401 -- The message digest of the data for a time stump, 402 -- A message digest algorithm identifier, 403 -- Message digest parameter, 404 -- The format of the document for a time stump, 405 -- The title of the document for a time stump, 406 -- The implementer of the document for a time stump, 407 -- The identifier of a public key certificate which performs an effectiveness check, 408 -- The time, 501 which perform the effectiveness check of a public key certificate -- Demand message reception time, 502 -- The data for a signature, 503 -- A public key certificate effectiveness check result, 504 -- The reason for a public key certificate invalid, 505 [-- Code data, 902 / -- The decode key, 903 which carried out

the code / -- A public key, 904 / -- A public-key-encryption algorithm identifier, 905 / -- Code data cryptographic algorithm identifier.] -- Public key certificate invalid time, 506 -- A public key certificate serial number, 507 -- The signature of a server, 901

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平10－105057
(43)公開日　平成10年(1998)４月24日

(51)Int.Cl.[6]	識別記号	FI	
G09C 1/00	640	G09C 1/00	640Z
			640D
G06F 13/00	351	G06F 13/00	351E

審査請求　未請求　請求項の数８　ＯＬ　（全９頁）

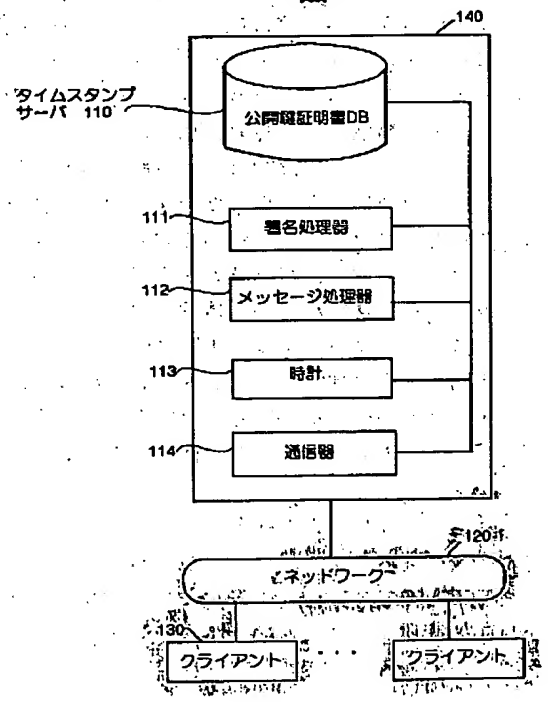
(21)出願番号　特願平8－253600
(22)出願日　平成８年(1996)９月25日

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地
(72)発明者　鮫島　吉喜
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内
(74)代理人　弁理士　秋田　収喜

(54)【発明の名称】タイムスタンプサーバシステム

(57)【要約】
【課題】　過去のある時点でコンピュータデータが既に存在してことを立証する証拠として用いることのできる情報の生成および使用すること。さらにメッセージの作成者／発信者／受信者、データを機密化し、第３者による情報の漏洩を防ぐこと。データやメッセージの送信・受信の証拠を残す書留機能や公証サービスを実現できること。
【解決手段】　データのメッセージダイジェストを生成するのに使用したアルゴリズムの識別子と付加的にパラメータを要求メッセージと返答メッセージ中のディジタル署名の対象データに含むようにした。また、データ、データのメッセージダイジェスト、データの作成者、電子メッセージの発信者や受信者の識別情報を暗号、復号鍵のメッセージダイジェストや復号鍵に対応する公開鍵と一緒に要求メッセージや返答メッセージを含めるようにした。

図1



1

【特許請求の範囲】

【請求項１】 複数のクライアントが接続され、特定のサービスを提供するタイムスタンプサーバから成るネットワークシステムにおいて、

クライアントのデータ送信に対して、タイムスタンプサーバは、データのメッセージダイジェストを生成するのに使用したアルゴリズムの識別子と付加的にパラメータを要求メッセージと返答メッセージ中のディジタル署名の対象データに含め、クライアントに返信することを特徴とするタイムスタンプサーバシステム。

【請求項２】 請求項１記載のタイムスタンプサーバシステムにおいて、

クライアントのデータ送信に対して、タイムスタンプサーバによる返信メッセージにデータのメッセージダイジェストと、

メッセージダイジェストを生成するのに使用したアルゴリズム識別子と、メッセージダイジェストを生成するのに使用した際のパラメータのいづれか1つか、もしくはそれぞれの組み合わせと、もしくは暗号した上記情報と暗号を復号する鍵のメッセージダイジェストと、鍵のメッセージダイジェスト生成に使用したアルゴリズムの識別子と、鍵のメッセージダイジェスト生成に使用したパラメータと、暗号に使用したアルゴリズムの識別子と、暗号に使用したパラメータのいづれか１つ、もしくはそれぞれの組み合わせと、もしくは暗号したデータと暗号を復号する鍵のメッセージダイジェストと、鍵のメッセージダイジェスト生成に使用したアルゴリズムの識別子と、鍵のメッセージダイジェスト生成に使用したパラメータと、暗号に使用したアルゴリズムの識別子と、暗号に使用したパラメータのいづれか一つかと、もしくはそれぞれの組み合わせと、もしくは上記暗号を復号する鍵を公開鍵を使って暗号化したデータと前記公開鍵と公開鍵暗号アルゴリズムのアルゴリズム識別子と、公開鍵暗号アルゴリズムのパラメータと、暗号に使用したアルゴリズムの識別子と、暗号に使用したパラメータのいづれか一つか、もしくはそれぞれの組み合わせのいずれかを含むクライアントからの要求メッセージに対して、時刻情報と、クライアントからの要求メッセージに含まれていた上記情報と、時刻情報とクライアントからの要求メッセージに含まれていた情報に対するディジタル署名とを含み、ディジタル署名生成に使用したアルゴリズムの識別子と、付加的にディジタル署名生成に使用したパラメータのいづれか、もしくは組み合わせを返答メッセージとして送信することを特徴とするタイムスタンプサーバシステム。

【請求項３】 請求項１または２記載のタイムスタンプサーバシステムにおいて、

時刻情報としてクライアントからの要求メッセージを受けた時刻、クライアントに送る返答メッセージ中のディジタル署名生成時刻、クライアントからの要求メッセージを受けた時刻のいづれか一つと、クライアントに送る返答メッセージ中のディジタル署名生成時刻を用いて、クライアントに返答メッセージを送信することを特徴とするタイムスタンプサーバシステム。

2

【請求項４】 請求項１または２記載のタイムスタンプサーバシステムにおいて、

クライアントからの要求メッセージの中にメッセージダイジェストの元となったデータの付属情報、付属情報のメッセージダイジェスト、暗号化した付属情報のいづれか一つか、もしくはそれぞれの組み合わせと、暗号を復号する鍵のメッセージダイジェストと、鍵のメッセージダイジェスト生成に使用したアルゴリズムの識別子と、鍵のメッセージダイジェスト生成に使用したパラメータと、暗号に使用したアルゴリズムの識別子と、暗号に使用したパラメータのいづれか一つか、もしくはそれぞれの組み合わせと、暗号した付属情報のメッセージダイジェストと、暗号を復号する鍵のメッセージダイジェストと、鍵のメッセージダイジェスト生成に使用したアルゴリズムの識別子と、鍵のメッセージダイジェスト生成に使用したパラメータと、暗号に使用したアルゴリズムの識別子と付加的に暗号に使用したパラメータのいづれかひとつか、もしくはそれぞれの組み合わせを含み、返答メッセージ中のディジタル署名の対象情報として、送信メッセージに含めて送信することを特徴とするタイムスタンプサーバシステム。

【請求項５】 請求項１または２記載のタイムスタンプサーバシステムにおいて、

サーバプログラムが、公開鍵暗号の公開鍵と前記公開鍵所有者の識別子を含む情報と、前記情報に対するディジタル署名を含む公開鍵証明書の有効性確認を行うことを特徴とするタイムスタンプサーバシステム。

【請求項６】 請求項１～５記載のいずれかのタイムスタンプサーバにおいて、サーバとクライアント間の要求メッセージと返答メッセージのやりとりをフロッピーディスクや磁気テープ、光ディスクなどの可搬データ格納媒体を利用してやりとりすることを特徴とするタイムスタンプサーバシステム。

【請求項７】 請求項１～６記載のいずれかのタイムスタンプサーバシステムにおいて、

タイムスタンプサーバからの返答情報に含まれるディジタル署名を検証することで、要求メッセージ中のメッセージダイジェストの元となったデータが返答メッセージ中の時刻情報より以前に存在していたことを立証することを特徴とするタイムスタンプサーバシステム。

【請求項８】 請求項１～７記載のいずれかのタイムスタンプサーバシステムにおいて、

返答メッセージのディジタル署名として公開鍵暗号もしくは秘密鍵暗号を利用することを特徴とするタイムスタンプサーバシステム。

【発明の詳細な説明】

3

【０００１】
【発明の属する技術分野】本発明は、ファイル、電子メッセージ、文書などのコンピュータデータが、ある日時に存在していたことの証明に関わる技術に係り、特に過去のある時点でコンピュータデータが既に存在してことを立証する証拠として用いることのできる情報の生成および使用に関するものである。
【０００２】
【従来の技術】タイムスタンプサービスの基本概念として、
ISO/IEC DIS 10181-4.2 Information technology — Open SystemsInterconnection — Security frameworks in Open Systems —Part 4: Non-repudiationがある。
【０００３】この基本概念に示されているタイムスタンプサーバへの要求メッセージにはデータもしくはデータのメッセージダイジェストが含まれていた。
【０００４】
【発明が解決しようとする課題】しかし、上記基本概念においてメッセージダイジェストを用いる場合、メッセージダイジェストを生成するのに用いたアルゴリズムの情報や生成の際のパラメータ情報を含んでいない。このため、データ存在の証拠である返答メッセージを検証する際、どのようにしてメッセージダイジェストが生成されたがわからない。
【０００５】また、本来メッセージダイジェストを生成したアルゴリズムとは異なるアルゴリズムを立証の際に使用してメッセージダイジェストを偽造し、実際には存在しなかったデータがある時点で存在していたと偽証することが可能であった。
【０００６】また、メッセージダイジェストからデータが特定される可能性があり、タイムスタンプ生成時にはタイムスタンプサーバに秘密にしておきたいデータのタイムスタンプの生成依頼ができなかった。
【０００７】また、上記基本概念ではデータの作成者やデータが電子メッセージであった場合の発信者や受信者情報を要求メッセージの中に含むことを示唆していた。このため、タイムスタンプサーバやタイムスタンプサーバの運営者にデータ作成者や電子メッセージの発信者／受信者が知られてしまうという問題があった。
【０００８】本発明の目的は、過去のある時点でコンピュータデータが既に存在してことを立証する証拠として用いることのできる情報の生成および使用することにあり、さらにメッセージの作成者／発信者／受信者、データを機密化し、第３者による情報の漏洩を防ぐことにある。たとえば、CALSや電子決済に際しては、単にデータや伝票、電子メッセージの暗号・認証だけでなく、データやメッセージの送信・受信の証拠を残す書留機能や公証サービスが、本発明の目的の一つになる。
【０００９】
【課題を解決するための手段】本発明では、データのメッセージダイジェストを生成するのに使用したアルゴリズムの識別子と付加的にパラメータを要求メッセージ中に含むようにし、サーバの返答メッセージ中の署名対象に識別子や付加的にパラメータを含めるようにした。

4

【００１０】さらに、データまたはデータのメッセージダイジェストを暗号、復号鍵のメッセージダイジェストも要求メッセージや返答メッセージに含め、復号鍵を公開鍵で暗号して結果の暗号データと公開鍵を含めた。
【００１１】また、データの作成者、電子メッセージの発信者や受信者の識別情報を暗号、復号鍵のメッセージダイジェストも要求メッセージや返答メッセージ含めた。
【００１２】
【発明の実施の形態】以下、本発明の一実施の形態を図面を用いて詳細に説明する。
【００１３】図１は本発明の全体構成を示す図である。
【００１４】タイムスタンプサービスシステム１４０は、タイムスタンプサーバ１１０、ネットワーク１２０、タイムスタンプサーバを利用する複数のクライアント１３０から構成される。タイムスタンプサーバ１１０は公開鍵証明書ＤＢ１１１、ディジタル署名処理器１１２、メッセージ処理器１１３、時計１１４、通信器１１５により構成される。
【００１５】タイムスタンプサーバ１１０は、クライアント１３０からの要求メッセージに対して、時刻情報を付加し、ディジタル署名を施した返答メッセージを返す。
【００１６】公開鍵証明書ＤＢ１１１は、国際標準X.509に代表される公開鍵証明書の情報を格納しているデータベースであり、メッセージ処理器１１３からの証明書状態問い合わせに対して、有効や無効、廃棄済みなどの返答を返す。無効の場合は、無効になった日時、理由を返すこともできる。
【００１７】署名生成器１１２はメッセージ処理器１１３からの依頼に対して、返答メッセージのディジタル署名を生成する。ディジタル署名の生成には、国際標準X.５０９にあるようなメッセージダイジェストと公開鍵暗号の技術を用いるのが一般的である。
【００１８】メッセージダイジェストとは、任意長のディジタルデータを一定長のデータに変換した結果であるが、以下のような様々な問題点がある。
【００１９】同じメッセージダイジェストを持つ異なるデータを捜し出すのは計算量的に困難であり、また、メッセージダイジェストから元のデータを推測するのは困難である。さらに、あるメッセージダイジェストになるデータを構成するのは困難であるという性質を持っている。
【００２０】また、ここで用いている公開鍵暗号とは暗号に用いる鍵と復号に用いる鍵が異なる暗号のことであり、対応する暗号鍵と復号鍵で暗号/復号しないと正し

5

く復号することができない。また、ディジタル署名は、この二つの技術を組み合わせることで、データの改竄検知やデータの作成元の真正性を検査している。

【００２１】メッセージ処理器１１３は、クライアントが送ってきた要求メッセージの解析や返答メッセージの生成を、他の構成要素を利用しながら行う。時計１１４は現在時刻を保持しており、メッセージ処理器１１３からの要求に対して現在時刻を返す。

【００２２】なお、本発明においては時刻の補正はタイムスタンプサーバの時計を基準にしており、各クライアントはこの時刻を基本としている。すべてのマシンの時刻の平均値を使用しても構わない。

【００２３】通信器１１５は、ネットワーク１２０を介して、タイムスタンプサーバ１１０とクライアント１３０間でやりとりされるメッセージの通信を処理してい

6

＊る。ネットワーク１２０は、タイムスタンプサーバ１１０とクライアント１３０を接続し、やりとりされる要求メッセージと返答メッセージを中継する。

【００２４】クライアント１３０は、データのメッセージダイジェストや、他の情報を含む要求データをタイムスタンプサーバ１１０に送信し、ディジタル署名のついた返答（メッセージタイムスタンプ証明書）を受けとる。返答メッセージは、サーバが要求メッセージを受信した時点で、メッセージダイジェストの元となったデータが存在したことを示す証拠として後日利用できるように保管する。

【００２５】要求メッセージには、表１に挙げるような情報のいくつかが含まれている。

【００２６】

【表１】

(1)存在証明が必要なデータのメッセージダイジェスト
(2)(1)に付加的につけられるメッセージダイジェストを生成するのに使用したメッセージアルゴリズムの識別子
(3)(1)に付加的につけられるメッセージダイジェストを生成するのに使用したアルゴリズムのパラメータ
(4)上記(1)(2)(3)メッセージダイジェストを生成するのに使用したアルゴリズムのパラメータ
(5)作成に使用した編集プログラムのファイルフォーマット識別情報、印刷用記述言語識別情報などのデータ形式を示す情報
(6)文書作成者
(7)文書の作成日時
(8)文書のタイトル
(9)文書識別番号
(10)電子メッセージの発信者
(11)電子メッセージの受信者
(12)電子メッセージの識別子

【００２７】図２は、データのメッセージダイジェスト、データの付属情報とも暗号された場合の要求メッセージを示す。

【００２８】データ２０１は、データのメッセージダイジェスト、付加的にメッセージダイジェストの生成アルゴリズム識別子と付加的にパラメータを暗号化した結果である。データ２０２は、項目２０１を復号する鍵のメッセージダイジェストである。項目２０３の「DES-CBC」は、データのメッセージダイジェスト他を暗号するのに使用したアルゴリズムの識別子である。２０４のデータは、データのメッセージダイジェストを暗号するのに使用したパラメータである。

【００２９】図３はサーバからクライアントへの返答メッセージの一例であり、図２の要求データに対する返答を示している。

【００３０】項目３０１の「１９９６０７１３１４２３４７」は、返答メッセージ中のディジタル署名３０３の生成日時が「１９９６年７月１３日１４時２３分４７秒」であることを示す。項目３０２は署名対象データである。項目３０３のデータは、項目３０１と項目３０２に対するサーバの署名である。項目３０４の「RSAEncryptionWithMD２」は、署名生成アルゴリズムを示す。項目３０５の「NULL」は、署名生成時にパラメータを使用しなかったことを示す。

【００３１】図４は、クライアントからサーバへの要求メッセージの一例である。

【００３２】項目４０１はデータのメッセージダイジェストである。項目４０２の「ＭＤ５」は、データのメッセージダイジェストを生成する時に使用したアルゴリズムの識別子である。項目４０３の「NULL」は、データのメッセージダイジェストを生成する時にパラメータを使用しなかったことを示す。次に示す項目４０４から項目４０８はデータの付加情報と公開鍵証明書の有効性確認情報の一例である。

【００３３】項目４０４の「Editer」は、データの文書の形式情報である。項目４０５の「タイムスタンプの特

許明細」は、データの文書タイトルである。項目４０６の「△立○之助」は、データの文書作成者名である。項目４０７の「３４５９」は、公開鍵証明書を識別するための情報であるシリアル番号である。項目４０８の「１９９６０６２２１７１１２９」は、公開鍵証明書の有効性確認をする日時が「１９９６年６月２２日１７時１１分２９秒」であることをを示す。

【００３４】図５は公開鍵証明書の有効性確認の情報、この場合、特に無効情報を含んだ返答メッセージを示す。

【００３５】項目５０１の「１９９６０７１３１４２３４５」は、「１９９６年７月１３日１４時２３分４５秒」にクライアントからの要求メッセージを受け付けたことを示す。項目５０２の署名対象データは、要求メッセージに含まれていたもので、この場合は図４に相当する。項目５０３は公開鍵証明書が無効になっていることを示す。５０４は無効になった理由を示す。項目５０５の「１９９６０６２１１２５６３４」は公開鍵に対応する個人鍵が「１９９６年６月２１日１２時５６分３４秒」に盗難にあったことを示す。項目５０６の「３４５９」は、無効になった公開鍵証明書を識別するためのシリアル番号である。項目５０７は項目５０１から項目５０６に対するサーバの署名である。

【００３６】以下、図６にしたがってタイムスタンプサーバ１１０の動作を詳細に説明する。

【００３７】通信器１１５は、クライアント１３０からネットワーク１２０を通じて送られてきた要求メッセージ（図２）を受信し、メッセージ処理器１３０に渡す（ステップ６０１）。

【００３８】メッセージ処理器１１３は、要求メッセージから署名対象データ２０１、２０２、２０３、２０４を取り出し、あらかじめ定められた情報のフォーマットに従っているかどうを検査する（ステップ６０２）。メッセージ処理器１１３は、時計１１４にアクセスし、現在時刻を得る（ステップ６０３）。

【００３９】メッセージ処理器１１３は、署名対象データ２０１、２０２、２０３、２０４、３０２と時刻情報を合わせて、署名処理器１１２に送る（ステップ６０４）。署名処理器１１２は、署名対象データと時刻情報からディジタル署名を生成し、メッセージ処理器１１３に返す（ステップ６０５）。

【００４０】メッセージ処理器１１３は、署名対象データ３０２、時刻情報３０１、ディジタル署名３０３、署名アルゴリズム３０４、パラメータ３０５から返答メッセージ（図３）を構成し、通信器１１５に渡す（ステップ６０６）。通信器１１５は、返答メッセージをクライアント１３０にネットワーク１２０を介して送る（ステップ６０７）。

【００４１】次に、図７を用いて公開鍵証明書確認サービスと組み合わせたタイムスタンプサービス処理を説明する。

【００４２】通信器１１５は、クライアント１３０からネットワーク１２０を通じて送られてきた要求メッセージを受信し、メッセージ処理器１３０に渡す（ステップ７０１）。メッセージ処理器１１３は、時計１１４にアクセスし、現在時刻を得る（ステップ７０２）。

【００４３】要求メッセージには、前記図４の例の他に加えて、次のような公開鍵証明書を識別するための情報が含まれる。発行した認証局Certification Authorityの識別子、シリアル番号、公開鍵public keyおよび個別鍵private keyの所有者、および有効性を確認する日時である。

【００４４】図４の要求メッセージでは、項目４０７にシリアル番号、項目４０８に有効性確認日時が含まれている。メッセージ処理器１１３は、上記情報を取り出し、あらかじめ定められた情報のフォーマットに従っているかどうかを検査する（ステップ７０３）。

【００４５】メッセージ処理器１１３は、公開鍵証明書ＤＢ１１１に上記公開鍵証明書の識別情報（項目４０７）と有効性を確認する日時情報（項目４０８）を送り、証明書の有効性を問い合わせる（ステップ７０４）。

【００４６】公開鍵証明書ＤＢ１１１は、証明書識別情報を元に検索し、有効性を確認する日時情報時点での公開鍵証明書の有効性を確認し、結果をメッセージ処理器１１３に返す（ステップ７０５）。確認の結果として有効や無効、無効の理由などがある。

【００４７】メッセージ処理器１１３は、署名対象データ４０１、４０２、４０３、４０４、４０５、４０６、４０７、４０９、４０８および５０２、証明書有効性確認結果と時刻情報を合わせて、署名処理器１１２に送る（ステップ７０６）。

【００４８】署名処理器１１２は、署名対象データと証明書有効性確認結果と時刻情報からディジタル署名を生成し、メッセージ処理器１１３に返す（ステップ７０７）。メッセージ処理器１１３は、署名対象データ５０２、時刻情報５０１、証明書有効性確認結果の無効５０３、無効理由５０４、無効日時５０５、証明書識別番号５０６とディジタル署名５０７からなる返答メッセージ（図５）を構成し、通信器１１５に渡す（ステップ７０８）。通信器１１５は、返答メッセージをクライアント１３０にネットワーク１２０を介して送る（ステップ７０９）。

【００４９】次に、図８を用いて返答メッセージ、すなわちタイムスタンプ証明書を用いた公証サービスを説明する。

【００５０】とくに、タイムスタンプサーバを運営するタイムスタンプサービス提供者とおよびタイムスタンプ証明書を用いて文書データが、ある時刻に存在したことを証明／保証するサービスの提供者とが国や地方公共団

体なら、裁判の証拠として採用することが将来可能になる。

【００５１】公証人は、証明希望者からタイムスタンプ証明書、対象データ、さらにタイムスタンプ証明書のデータのメッセージダイジェストが暗号されている場合には復号の鍵を受け取る（ステップ８０１）。

【００５２】タイムスタンプ証明書のディジタル署名が正しいかどうかを確認する。特に、署名として公開鍵証明書を使っている場合には、タイムスタンプサーバの公開鍵を使って署名を確認する（ステップ８０２）。タイムスタンプ証明書に含まれるデータのメッセージダイジェストが暗号されている場合、受け取った復号鍵のメッセージダイジェストとタイムスタンプ証明書の中の復号鍵のメッセージダイジェストとが一致することを確認する（ステップ８０３）。

【００５３】タイムスタンプ証明書に含まれるデータのメッセージダイジェストが暗号されている場合、復号鍵を使って復号し、データのメッセージダイジェストを得る（ステップ８０４）。

【００５４】受け取ったデータのメッセージダイジェストを計算し、タイムスタンプ証明書から得たデータのメッセージダイジェストと一致することを確認する。一致すれば、ダイムスタンプ証明書に含まれる時刻以前に当該データが存在していたことを保証する（ステップ８０５）。

【００５５】図９および１０を用いて公開鍵暗号を使った場合の本発明の実施の形態について説明する。

【００５６】項目９０１は暗号した文書など署名対象になるデータである。暗号には通常、秘密鍵対称鍵暗号を用いる。項目９０２は、項目９０１のデータを復号する鍵を暗号したものである。暗号には公開鍵暗号を用いる。項目９０３は、項目９０２の暗号に用いた公開鍵である。項目９０４は公開鍵暗号のアルゴリズムの識別子である。項目９０５は、項目９０１のデータを暗号したアルゴリズムの識別子である。図９の要求メッセージのタイムスタンプサーバの返答メッセージは図３に記載されており、処理は図６と同様なので省略する。返答メッセージの署名対象データ３０２が要求メッセージ（図９）に対応する。

【００５７】次に、図１０を用いて公開鍵を用いた場合の公証サービスを説明する。

【００５８】公証人は証明希望者からタイムスタンプ証明書、つまり図９の要求メッセージに対する返答メッセージ図３と公開鍵に対応する個別鍵を受け取る（ステップ１００１）。

【００５９】次に、タイムスタンプ証明書のディジタル署名が正しいかどうかを確認する（ステップ１００２）。確認の方法は、前述のステップ８０２と同様である。次に、ダイムスタンプ証明書に含まれる公開鍵と受け取った個別鍵が対応しているかどうか確認する（ステップ１００３）。公開鍵はタイムスタンプ、すなわち返答メッセージ（図３）の項目３０２に対応する図９の要求メッセージの項目９０３と同じである。

【００６０】個別鍵を使って暗号した復号鍵（図９の要求メッセージの９０２と同じ）を復号することでデータ復号鍵が得られる。復号に使うアルゴリズムは、９０４に当たる識別子に対応する公開鍵暗号アルゴリズムである。得られた復号鍵で（暗号データ；項目９０１）を復号し署名対象データを得る（ステップ１００５）。復号に使うアルゴリズムは、要求メッセージ９０５にあった識別子に対応するアルゴリズムである。

【００６１】これにより、タイムスタンプ証明書に含まれる時刻以前にデータが存在していたことが証明できる。

【００６２】

【発明の効果】以上のように本発明では、存在の証拠が必要なデータからメッセージダイジェストを作成する際に使用したアルゴリズムの識別子や付加的にパラメータを要求メッセージ含めるようにし、タイムスタンプサーバはこれらの情報を元にディジタル署名をしている。このため、どのようなアルゴリズムを用いてメッセージダイジェストを生成したか、証拠である返答メッセージに含まれているため、どのようにして証拠を検証すればいいのかがわかる。また、実際にデータのメッセージダイジェストを生成した方法とは別の方法で検証時にメッセージダイジェストを作成することが防げるので、偽証を防ぐことができる。

【００６３】また、データのメッセージダイジェストの代わりに暗号したデータのメッセージダイジェストを署名対象データとすることで、タイムスタンプ生成時にはサーバに秘密にしておきたいデータに対しでもタイムスタンプサーバに依頼することが可能となる。　また、別の手段としてデータを暗号して復号鍵のメッセージダイジェストを含め、復号鍵を公開鍵で暗号した時も同様の効果が得ることができる。

【００６４】また、データの作成者、電子メッセージの発信者や受信者の識別情報を暗号して要求メッセージや返答メッセージを含めるようにしたので、タイムスタンプサーバやタイムスタンプサーバの運営者に知られることなくデータ作成者や電子メッセージの発信者・受信者を含めたデータの付加情報に対してタイムスタンプサーバの署名をもらうことが可能となる。

【図面の簡単な説明】

【図１】タイムスタンプサービスの全体構成、およびタイムスタンプサーバの内部構成図である。

【図２】メッセージダイジェストを含む要求メッセージ構成図である。

【図３】図２の要求メッセージに対する返答メッセージ構成図である。

【図４】暗号したメッセージダイジェストを含む要求メ

ッセージ構成図である。

【図５】図４の要求メッセージに対する返答メッセージ構成図である。

【図６】タイムスタンプサーバの基本動作を示すフローチャートである。

【図７】公開鍵証明書の有効性確認サービスと組み合わせた場合のタイムスタンプサーバの動作を示すフローチャートである。

【図８】タイムスタンプ証明書を用いたデータの存在を確認する証明者公証人の動作を示すフローチャートである。

【図９】請求項１で公開鍵を使った場合の要求メッセージ構成図である。

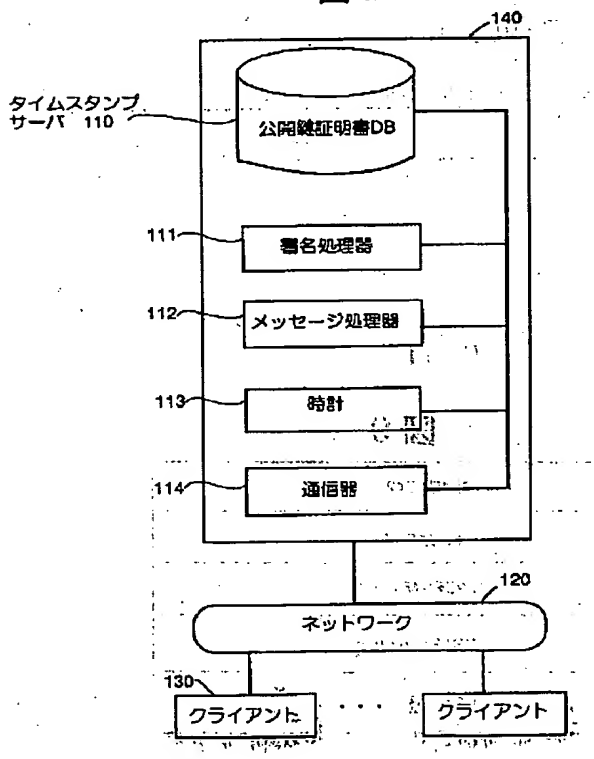
【図１０】請求項１で公開鍵を使った場合のデータの存在を確認する証明者公証人の動作を示すフローチャートである。

【符号の説明】

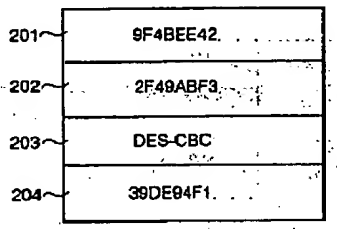
１１０…タイムスタンプサーバ、１１１…公開鍵証明書DB、１１２…ディジタル署名処理器、１１３…要求・返答メッセージ処理器、１１４…時計、１１５…通信器、１２０…ネットワーク、１３０…クライアント、１４０…タイムスタンプサービスシステム、２０１…タイムス

タンプ対象データのメッセージダイジェスト及び付加的にアルゴリズムとパラメータを暗号した結果、２０２…201を復号する鍵のメッセージダイジェスト、２０３…201の暗号に使用したアルゴリズムの識別子、２０４…201の暗号に使用したパラメータ、３０１…ディジタル署名の生成日時、３０２…証明対象データ、３０３…サーバの署名、３０４…署名生成アルゴリズム識別子、３０５…署名生成パラメータ、４０１…タイムスタンプ対象データのメッセージダイジェスト、４０２…メッセージダイジェストアルゴリズム識別子、４０３…メッセージダイジェストパラメータ、４０４…タイムスタンプ対象文書の形式、４０５…タイムスタンプ対象文書のタイトル、４０６…タイムスタンプ対象文書の作成者、４０７…有効性確認を行う公開鍵証明書の識別子、４０８…公開鍵証明書の有効性確認を行う日時、５０１…要求メッセージ受付日時、５０２…署名対象データ、５０３…公開鍵証明書有効性確認結果、５０４…公開鍵証明書無効理由、５０５…公開鍵証明書無効日時、５０６…公開鍵証明書シリアル番号、５０７…サーバの署名、９０１…暗号データ、９０２…暗号した復号鍵、９０３…公開鍵、９０４…公開鍵暗号アルゴリズム識別子、９０５…暗号データ暗号アルゴリズム識別子。

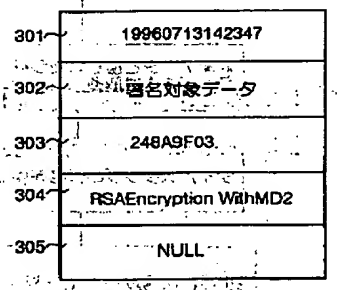
【図１】



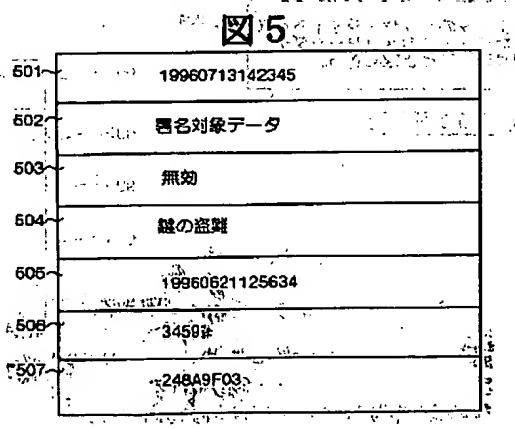
【図２】



【図３】

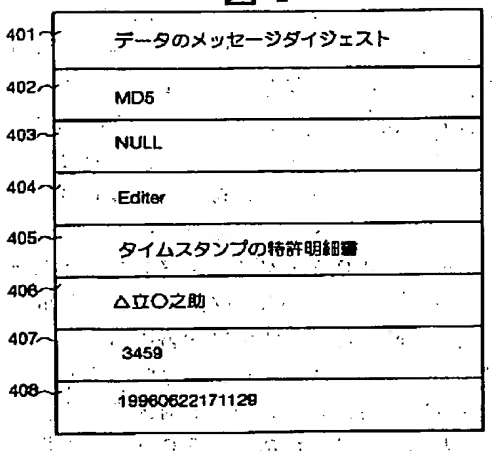


【図５】



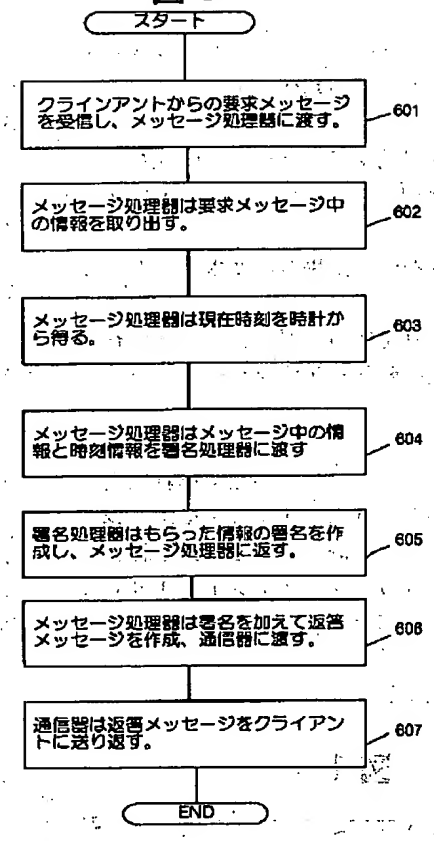
【図４】

図４



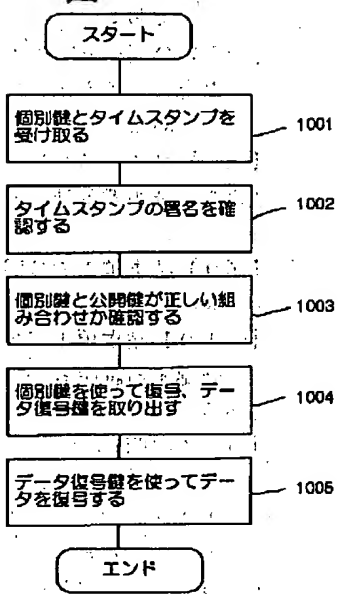
【図６】

図６



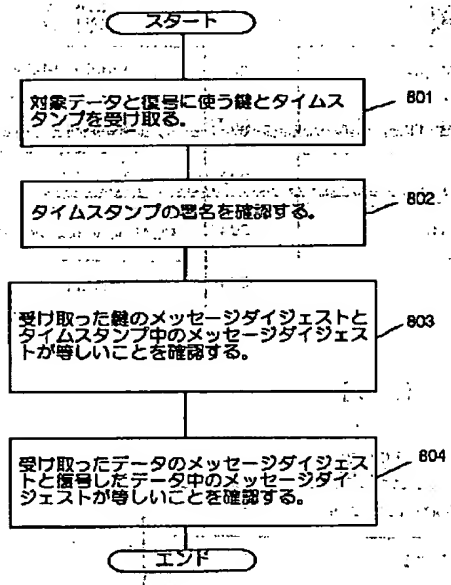
【図１０】

図１０



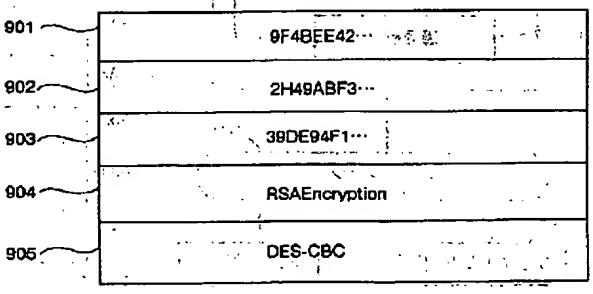
【図８】

図８



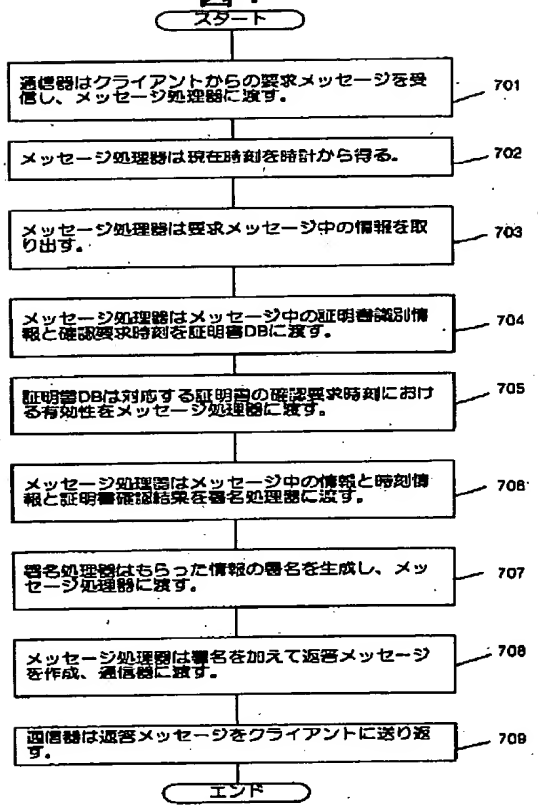
【図９】

図９



【図7】

図7


スタート
通信器はクライアントからの要求メッセージを受信し、メッセージ処理器に渡す。
701
メッセージ処理器は現在時刻を時計から得る。
702
メッセージ処理器は要求メッセージ中の情報を取り出す。
703
メッセージ処理器はメッセージ中の証明書識別情報と確認要求時刻を証明書DBに渡す。
704
証明書DBは対応する証明書の確認要求時刻における有効性をメッセージ処理器に渡す。
705
メッセージ処理器はメッセージ中の情報と時刻情報と証明書確認結果を署名処理器に渡す。
706
署名処理器はもらった情報の署名を生成し、メッセージ処理器に渡す。
707
メッセージ処理器は署名を加えて返答メッセージを作成、通信器に渡す。
708
通信器は返答メッセージをクライアントに送り返す。
709
エンド

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成１１年（１９９９）１１月２６日

【公開番号】特開平１０－１０５０５７
【公開日】平成１０年（１９９８）４月２４日
【年通号数】公開特許公報１０－１０５１
【出願番号】特願平８－２５３６００
【国際特許分類第６版】
G09C 1/00 640
G06F 13/00 351
【ＦＩ】
G09C 1/00 640 Z
640 D
G06F 13/00 351 E

【手続補正書】
【提出日】平成１１年３月３０日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】全文
【補正方法】変更
【補正内容】
【書類名】　明細書
【発明の名称】　タイムスタンプサーバシステム
【特許請求の範囲】
【請求項１】　複数のクライアントが接続され、特定のサービスを提供するタイムスタンプサーバから成るネットワークシステムにおいて、
前記クライアントのそれぞれが、タイムスタンプサービス要求として、対象となるデータのメッセージダイジェストの他に、該メッセージダイジェストを生成するのに使用したアルゴリズムの識別子とパラメータを要求メッセージ中に付加的に含めて前記タイムスタンプサーバに送信する手段を備え、
前記タイムスタンプサーバが、前記クライアントからの要求メッセージ中の前記アルゴリズムの識別子とパラメータをディジタル署名の対象データに付加的に含めて返答メッセージを生成し、要求元のクライアントに返信する手段を備えることを特徴とするタイムスタンプサーバシステム。
【請求項２】　請求項１記載のタイムスタンプサーバシステムにおいて、
クライアントのデータ送信に対して、タイムスタンプサーバによる返信メッセージにデータのメッセージダイジェストと、
メッセージダイジェストを生成するのに使用したアルゴリズム識別子と、メッセージダイジェストを生成するのに使用した際のパラメータのいづれか１つか、もしくはそれぞれの組み合わせと、もしくは暗号化した上記情報と暗号を復号する鍵のメッセージダイジェストと、鍵のメッセージダイジェスト生成に使用したアルゴリズムの識別子と、鍵のメッセージダイジェスト生成に使用したパラメータと、暗号に使用したアルゴリズムの識別子と、暗号に使用したパラメータのいづれか１つ、もしくはそれぞれの組み合わせと、もしくは暗号したデータと暗号を復号する鍵のメッセージダイジェストと、鍵のメッセージダイジェスト生成に使用したアルゴリズムの識別子と、鍵のメッセージダイジェスト生成に使用したパラメータと、暗号に使用したアルゴリズムの識別子と、暗号に使用したパラメータのいづれか一つかと、もしくはそれぞれの組み合わせと、もしくは上記暗号を復号する鍵を公開鍵を使って暗号化したデータと前記公開鍵と公開鍵暗号アルゴリズムのアルゴリズム識別子と、公開鍵暗号アルゴリズムのパラメータと、暗号に使用したアルゴリズムの識別子と、暗号に使用したパラメータのいづれか一つか、もしくはそれぞれの組み合わせのいずれかを含むクライアントからの要求メッセージに対して、時刻情報と、クライアントからの要求メッセージに含まれていた上記情報と、時刻情報とクライアントからの要求メッセージに含まれていた情報に対するディジタル署名とを含み、ディジタル署名生成に使用したアルゴリズムの識別子と、付加的にディジタル署名生成に使用したパラメータのいづれか、もしくは組み合わせを返答メッセージとして送信する手段を備えることを特徴とするタイムスタンプサーバシステム。
【請求項３】　請求項１または２記載のタイムスタンプサーバシステムにおいて、
時刻情報としてクライアントからの要求メッセージを受けた時刻、クライアントに送る返答メッセージ中のディジタル署名生成時刻、クライアントからの要求メッセー

ジを受けた時刻のいづれか一つと、クライアントに送る返答メッセージ中のディジタル署名生成時刻を用いて、クライアントに返答メッセージを送信する手段を備えることを特徴とするタイムスタンプサーバシステム。

【請求項４】　請求項１または２記載のタイムスタンプサーバシステムにおいて、

クライアントからの要求メッセージの中にメッセージダイジェストの元となったデータの付属情報、付属情報のメッセージダイジェスト、暗号化した付属情報のいづれか一つか、もしくはそれぞれの組み合わせと、暗号を復号する鍵のメッセージダイジェストと、鍵のメッセージダイジェスト生成に使用したアルゴリズムの識別子と、鍵のメッセージダイジェスト生成に使用したパラメータと、暗号に使用したアルゴリズムの識別子と、暗号に使用したパラメータのいづれか一つか、もしくはそれぞれの組み合わせと、暗号化した付属情報のメッセージダイジェストと、暗号を復号する鍵のメッセージダイジェストと、鍵のメッセージダイジェスト生成に使用したアルゴリズムの識別子と、鍵のメッセージダイジェスト生成に使用したパラメータと、暗号に使用したアルゴリズムの識別子と付加的に暗号に使用したパラメータのいづれかひとつか、もしくはそれぞれの組み合わせを含み、返答メッセージ中のディジタル署名の対象情報として、送信メッセージに含めて送信する手段を備えることを特徴とするタイムスタンプサーバシステム。

【請求項５】　請求項１または２記載のタイムスタンプサーバシステムにおいて、

サーバプログラムが、公開鍵暗号の公開鍵と前記公開鍵所有者の識別子を含む情報と、前記情報に対するディジタル署名を含む公開鍵証明書の有効性確認を行うことを特徴とするタイムスタンプサーバシステム。

【請求項６】　請求項１～５記載のいずれかのタイムスタンプサーバにおいて、

サーバとクライアント間の要求メッセージと返答メッセージのやりとりをフロッピーディスクや磁気テープ、光ディスクなどの可搬データ格納媒体を利用してやりとりすることを特徴とするタイムスタンプサーバシステム。

【請求項７】　請求項１～６記載のいずれかのタイムスタンプサーバシステムにおいて、

タイムスタンプサーバからの返答情報に含まれるディジタル署名を検証することで、要求メッセージ中のメッセージダイジェストの元となったデータが返答メッセージ中の時刻情報より以前に存在していたことを立証することを特徴とするタイムスタンプサーバシステム。

【請求項８】　請求項１～７記載のいずれかのタイムスタンプサーバシステムにおいて、

返答メッセージのディジタル署名として公開鍵暗号もしくは秘密鍵暗号を利用することを特徴とするタイムスタンプサーバシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ファイル、電子メッセージ、文書などのコンピュータデータが、ある日時に存在していたことの証明に関わる技術に係り、特に過去のある時点でコンピュータデータが既に存在してことを立証する証拠として用いることのできる情報の生成および使用方法に関するものである。

【０００２】

【従来の技術】タイムスタンプサービスの基本概念として、ISO/IEC DIS 10181-4.2 Information technology -- Open Systems Interconnection -- Security frameworks in Open Systems --Part 4: Non-repudiationがある。

【０００３】この基本概念に示されているタイムスタンプサーバへの要求メッセージにはデータもしくはデータのメッセージダイジェストが含まれていた。メッセージダイジェストとは、任意長のディジタルデータを一定長のデータに変換した結果のことである。

【０００４】

【発明が解決しようとする課題】しかし、上記基本概念においてメッセージダイジェストを用いる場合、メッセージダイジェストを生成するのに用いたアルゴリズムの情報や生成の際のパラメータ情報を含んでいない。このため、データ存在の証拠である返答メッセージを検証する際、どのようにしてメッセージダイジェストが生成されたのかがわからない。

【０００５】また、本来メッセージダイジェストを生成したアルゴリズムとは異なるアルゴリズムを立証の際に使用してメッセージダイジェストを偽造し、実際には存在しなかったデータがある時点で存在していたと偽証することが可能であった。

【０００６】また、メッセージダイジェストからデータが特定される可能性があり、タイムスタンプ生成時にはタイムスタンプサーバに秘密にしておきたいデータのタイムスタンプの生成依頼ができなかった。

【０００７】また、上記基本概念ではデータの作成者の情報やデータが電子メッセージであった場合の発信者や受信者情報を要求メッセージの中に含むことを示唆していた。このため、タイムスタンプサーバやタイムスタンプサーバの運営者にデータ作成者や電子メッセージの発信者／受信者が知られてしまうという問題があった。

【０００８】本発明の目的は、過去のある時点でコンピュータデータが既に存在したことを立証する証拠として用いることのできる情報の生成および使用方法を実現することにあり、さらにメッセージの作成者／発信者／受信者、データを機密化し、第３者による情報の漏洩を防ぐことにある。たとえば、CALSや電子決済に際しては、単にデータや伝票、電子メッセージの暗号・認証だけでなく、データやメッセージの送信・受信の証拠を残す書留機能や公証サービスが、本発明の目的の一つになる。

【０００９】

【課題を解決するための手段】本発明では、データのメッセージダイジェストを生成するのに使用したアルゴリズムの識別子の他に、付加的にパラメータを要求メッセージ中に含むようにし、サーバの返答メッセージ中の署名対象に識別子やパラメータを付加的に含めるようにした。

【００１０】

【発明の実施の形態】以下、本発明の一実施の形態を図面を用いて詳細に説明する。

【００１１】図１は本発明の全体構成を示す図である。

【００１２】タイムスタンプサービスシステム１４０は、タイムスタンプサーバ１１０、ネットワーク１２０、タイムスタンプサーバを利用する複数のクライアント１３０から構成される。タイムスタンプサーバ１１０は公開鍵証明書ＤＢ１１１、ディジタル署名処理器１１２、メッセージ処理器１１３、時計１１４、通信器１１５により構成される。

【００１３】タイムスタンプサーバ１１０は、クライアント１３０からの要求メッセージに対して、時刻情報を付加し、ディジタル署名を施した返答メッセージを返す。

【００１４】公開鍵証明書D.B１１１は、国際標準X.５０９に代表される公開鍵証明書の情報を格納しているデータベースであり、メッセージ処理器１１３からの証明書状態問い合わせに対して、有効や無効、廃棄済みなどの返答を返す。無効の場合は、無効になった日時、理由を返すこともできる。

【００１５】署名生成器１１２はメッセージ処理器１１３からの依頼に対して、返答メッセージのディジタル署名を生成する。ディジタル署名の生成には、国際標準X.５０９にあるようなメッセージダイジェストと公開鍵暗号の技術を用いるのが一般的である。

【００１６】メッセージダイジェストとは、任意長のディジタルデータを一定長のデータに変換した結果であるが、以下のような様々な性質を持っている。

【００１７】同じメッセージダイジェストを持つ異なるデータを捜し出すのは計算量的に困難であり、また、メッセージダイジェストから元のデータを推測するのは困難である。さらに、あるメッセージダイジェストになるデータを構成するのは困難であるという性質を持っている。

【００１８】また、ここで用いている公開鍵暗号とは暗号化に用いる鍵と復号に用いる鍵が異なる暗号のことであり、対応する暗号鍵と復号鍵で暗号/復号しないと正しく復号することができない。また、ディジタル署名は、この二つの技術を組み合わせることで、データの改竄検知やデータの作成元の真正性を検査している。

【００１９】メッセージ処理器１１３は、クライアント１３０が送ってきたタイムスタンプの要求メッセージの解析や、その要求メッセージに対する返答メッセージの生成を、タイムスタンプサーバ１１０内の他の構成要素を利用しながら行う。時計１１４は現在時刻を保持しており、メッセージ処理器１１３からの要求に対して現在時刻を返す。

【００２０】なお、本発明においては時刻の補正はタイムスタンプサーバ１１０の時計を基準にしており、各クライアント１３０はこの時刻を基本としている。すべてのマシン（クライアント）の時刻の平均値を使用しても構わない。

【００２１】通信器１１５は、ネットワーク１２０を介して、タイムスタンプサーバ１１０とクライアント１３０間でやりとりされるメッセージの通信を処理している。ネットワーク１２０は、タイムスタンプサーバ１１０とクライアント１３０を接続し、やりとりされる要求メッセージと返答メッセージを中継する。

【００２２】クライアント１３０は、データのメッセージダイジェストや、他の情報を含む要求データをタイムスタンプサーバ１１０に送信し、ディジタル署名のついた返答（メッセージタイムスタンプ証明書）を受けとる。返答メッセージは、サーバ１１０が要求メッセージを受信した時点で、メッセージダイジェストの元となったデータが存在したことを示す証拠として後日利用できるように保管される。

【００２３】要求メッセージには、表１に挙げるような情報のいくつかが含まれている。

【００２４】

【表１】

(4)

5 6

(1)存在証明が必要なデータのメッセージダイジェスト (2)(1)に付加的につけられるメッセージダイジェストを生成するのに使用したメッセージアルゴリズムの識別子 (3)(1)に付加的につけられるメッセージダイジェストを生成するのに使用したアルゴリズムのパラメータ
(4)上記(1)(2)(3)メッセージダイジェストを生成するのに使用したアルゴリズムのパラメータ
(5)作成に使用した編集プログラムのファイルフォーマット識別情報、印刷用記述言語識別情報などのデータ形式を示す情報 (6)文書作成者 (7)文書の作成日時 (8)文書のタイトル (9)文書識別番号 (10)電子メッセージの発信者 (11)電子メッセージの受信者 (12)電子メッセージの識別子

【００２５】図２は、データのメッセージダイジェスト、データの付属情報とも暗号化された場合のタイムスタンプの要求メッセージを示す。

【００２６】データ２０１は、データのメッセージダイジェスト、付加的にメッセージダイジェストの生成アルゴリズム識別子と付加的にパラメータを暗号化した結果である。データ２０２は、項目２０１を復号する鍵のメッセージダイジェストである。項目２０３の「DES-CBC」は、データのメッセージダイジェスト他を暗号化するのに使用したアルゴリズムの識別子である。２０４のデータは、データのメッセージダイジェストを暗号化するのに使用したパラメータである。

【００２７】図３はタイムスタンプサーバ１１０からクライアント１３０への返答メッセージの一例であり、図２の要求データに対する返答を示している。

【００２８】項目３０１の「１９９６０７１３１４２３４７」は、返答メッセージ中のディジタル署名３０３の生成日時が「１９９６年７月１３日１４時２３分４７秒」であることを示す。項目３０２は署名対象データである。署名対象データとは、図２の２０１から２０４のデータのことである。項目３０３のデータは、項目３０１と項目３０２に対するタイムスタンプサーバ１１０の署名である。項目３０４の「RSAEncryptionWithMD２」は、署名生成アルゴリズムを示す。項目３０５の「NULL」は、署名生成時にパラメータを使用しなかったことを示す。

【００２９】図４は、クライアント１３０からタイムスタンプサーバ１１０への要求メッセージの一例である。

【００３０】項目４０１はデータのメッセージダイジェストである。項目４０２の「ＭＤ５」は、データのメッセージダイジェストを生成する時に使用したアルゴリズムの識別子である。項目４０３の「NULL」は、データのメッセージダイジェストを生成する時にパラメータを使用しなかったことを示す。次に示す項目４０４から項目４０８はデータの付加情報と公開鍵証明書の有効性確認情報の一例である。

【００３１】項目４０４の「Editer」は、データの文書の形式情報である。項目４０５の「タイムスタンプの特許明細」は、データの文書タイトルである。項目４０６の「△立○之助」は、データの文書作成者名である。項目４０７の「３４５９」は、公開鍵証明書を識別するための情報であるシリアル番号である。項目４０８の「１９９６０６２２１７１１２９」は、公開鍵証明書の有効性確認をする日時が「１９９６年６月２２日１７時１１分２９秒」であることを示す。

【００３２】図５は公開鍵証明書の有効性確認の情報、この場合、特に無効情報を含んだ返答メッセージを示す。

【００３３】項目５０１の「１９９６０７１３１４２３４５」は、「１９９６年７月１３日１４時２３分４５秒」にクライアントからの要求メッセージを受け付けたことを示す。項目５０２の署名対象データは、要求メッセージに含まれていたもので、この場合は図４の全部に相当する。項目５０３は図４の４０７で識別される公開鍵証明書が無効になっていることを示す。５０４は無効になった理由を示す。項目５０５の「１９９６０６２１１２５６３４」は公開鍵に対応する個人鍵が「１９９６年６月２１日１２時５６分３４秒」に盗難にあったことを示す。項目５０６の「３４５９」は、無効になった公開鍵証明書を識別するためのシリアル番号である。項目５０７は項目５０１から項目５０６に対するタイムスタンプサーバ１１０の署名である。

【００３４】以下、図６にしたがってタイムスタンプサーバ１１０の動作を詳細に説明する。

【００３５】通信器１１５は、クライアント１３０からネットワーク１２０を通じて送られてきたタイムスタン

7

プの要求メッセージ（図２）を受信し、メッセージ処理器１３０に渡す（ステップ６０１）。

【００３６】メッセージ処理器１１３は、要求メッセージから署名対象データ２０１、２０２、２０３、２０４を取り出し、あらかじめ定められた情報のフォーマットに従っているかどうを検査する（ステップ６０２）。メッセージ処理器１１３は、時計１１４にアクセスし、現在時刻を得る（ステップ６０３）。

【００３７】メッセージ処理器１１３は、署名対象データ２０１、２０２、２０３、２０４と時刻情報を合わせて、署名処理器１１２に送る（ステップ６０４）。署名処理器１１２は、署名対象データと時刻情報からディジタル署名を生成し、メッセージ処理器１１３に返す（ステップ６０５）。

【００３８】メッセージ処理器１１３は、署名対象データ３０２（２０１、２０２、２０３、２０４に相当）、時刻情報３０１、ディジタル署名３０３、署名アルゴリズム３０４、パラメータ３０５から返答メッセージ（図３）を構成し、通信器１１５に渡す（ステップ６０６）。通信器１１５は、返答メッセージをクライアント１３０にネットワーク１２０を介して送る（ステップ６０７）。

【００３９】次に、図７を用いて公開鍵証明書確認サービスと組み合わせたタイムスタンプサービス処理を説明する。

【００４０】通信器１１５は、クライアント１３０からネットワーク１２０を通じて送られてきた要求メッセージを受信し、メッセージ処理器１１３に渡す（ステップ７０１）。メッセージ処理器１１３は、時計１１４にアクセスし、現在時刻を得る（ステップ７０２）。

【００４１】要求メッセージには、前記図４の例の他に加えて、次のような公開鍵証明書を識別するための情報が含まれる。発行した認証局Certification Authorityの識別子、シリアル番号、公開鍵public keyおよび個別鍵private keyの所有者、および有効性を確認する日時である。

【００４２】図４の要求メッセージでは、項目４０７にシリアル番号、項目４０８に有効性確認日時が含まれている。メッセージ処理器１１３は、上記情報を取り出し、あらかじめ定められた情報のフォーマットに従っているかどうかを検査する（ステップ７０３）。

【００４３】メッセージ処理器１１３は、公開鍵証明書ＤＢ１１１に上記公開鍵証明書の識別情報（項目４０７）と有効性を確認する日時情報（項目４０８）を送り、証明書の有効性を問い合わせる（ステップ７０４）。

【００４４】公開鍵証明書ＤＢ１１１は、証明書識別情報を元に検索し、有効性を確認する日時情報時点での公開鍵証明書の有効性を確認し、結果をメッセージ処理器１１３に返す（ステップ７０５）。確認の結果として有効や無効、無効の理由などがある。

8

【００４５】メッセージ処理器１１３は、署名対象データ４０１、４０２、４０３、４０４、４０５、４０６、４０７、４０９、４０８、証明書有効性確認結果と時刻情報を合わせて、署名処理器１１２に送る（ステップ７０６）。

【００４６】署名処理器１１２は、署名対象データ５０２（４０１、４０２、４０３、４０４、４０５、４０６、４０７、４０９、４０８に相当）と証明書有効性確認結果５０３～５０６と時刻情報５０１からディジタル署名５０７を生成し、メッセージ処理器１１３に返す（ステップ７０７）。メッセージ処理器１１３は、署名対象データ５０２、時刻情報５０１、証明書有効性確認結果の無効５０３、無効理由５０４、無効日時５０５、証明書識別番号５０６とディジタル署名５０７からなる返答メッセージ（図５）を構成し、通信器１１５に渡す（ステップ７０８）。通信器１１５は、返答メッセージをクライアント１３０にネットワーク１２０を介して送る（ステップ７０９）。

【００４７】次に、図８を用いて返答メッセージ、すなわちタイムスタンプ証明書を用いた公証サービスを説明する。

【００４８】タイムスタンプサーバを運営するタイムスタンプサービス提供者と、タイムスタンプ証明書を用いた文書データについてその文書データが「ある時刻に存在したことを証明／保証するサービス」の提供者とが国や地方公共団体なら、裁判の証拠として採用することが将来可能になる。

【００４９】公証人は、証明希望者からタイムスタンプ証明書、対象データ、さらにタイムスタンプ証明書のデータのメッセージダイジェストが暗号化されている場合には復号の鍵を受け取る（ステップ８０１）。

【００５０】次に、タイムスタンプ証明書のディジタル署名が正しいかどうかを確認する。特に、署名として公開鍵証明書を使っている場合には、タイムスタンプサーバ１１０の公開鍵を使って署名を確認する（ステップ８０２）。タイムスタンプ証明書に含まれるデータのメッセージダイジェストが暗号化されている場合、受け取った復号鍵のメッセージダイジェストとタイムスタンプ証明書の中の復号鍵のメッセージダイジェスト（図２の２０２に相当）とが一致することを確認する（ステップ８０３）。

【００５１】タイムスタンプ証明書に含まれるデータのメッセージダイジェストが暗号化されている場合、復号鍵を使って復号し、データのメッセージダイジェストを得る。この復号は図２の２０３，２０４にあるアルゴリズム、パラメータを用いる。

【００５２】受け取ったデータのメッセージダイジェストを計算し、タイムスタンプ証明書から得たデータのメッセージダイジェストと一致することを確認する。一致

すれば、ダイムスタンプ証明書に含まれる時刻以前に当該データが存在していたことを保証する（ステップ８０４）。

【００５３】図９および１０を用いて公開鍵暗号を使った場合の本発明の実施の形態について説明する。

【００５４】項目９０１は暗号化した文書など署名対象になるデータである。暗号には通常、秘密鍵暗号を用いる。項目９０２は、項目９０１のデータを復号する鍵を暗号化したものである。暗号化には公開鍵暗号を用いる。項目９０３は、項目９０２の暗号に用いた公開鍵である。項目９０４は公開鍵暗号のアルゴリズムの識別子である。項目９０５は、項目９０１のデータを暗号化したアルゴリズムの識別子である。図９の要求メッセージのタイムスタンプサーバの返答メッセージは図３に記載されており、処理は図６と同様なので省略する。返答メッセージの署名対象データ３０２が要求メッセージ（図９）に対応する。

【００５５】次に、図１０を用いて公開鍵を用いた場合の公証サービスを説明する。

【００５６】公証人は証明希望者からタイムスタンプ証明書、つまり図９の要求メッセージに対する返答メッセージ（図３）と公開鍵に対応する個別鍵を受け取る（ステップ１００１）。

【００５７】次に、タイムスタンプ証明書のディジタル署名が正しいかどうかを確認する（ステップ１００２）。確認の方法は、前述のステップ８０２と同様である。次に、タイムスダンプ証明書に含まれる公開鍵と受け取った個別鍵が対応しているかどうか確認する（ステップ１００３）。公開鍵はタイムスタンプ、すなわち返答メッセージ（図３）の項目３０２に対応する図９の要求メッセージの項目９０３と同じである。

【００５８】個別鍵を使って暗号した復号鍵（図９の要求メッセージの９０２と同じ）を復号することでデータ復号鍵が得られる。復号に使うアルゴリズムは、９０４に当たる識別子に対応する公開鍵暗号アルゴリズムである。得られた復号鍵で暗号データ（項目９０１）を復号し署名対象データを得る（ステップ１００５）。復号に使うアルゴリズムは、要求メッセージ９０５にあった識別子に対応するアルゴリズムである。

【００５９】これにより、タイムスタンプ証明書に含まれる時刻以前にデータが存在していたことが証明できる。

【００６０】

【発明の効果】以上のように本発明では、存在の証拠が必要なデータからメッセージダイジェストを作成する際に使用したアルゴリズムの識別子やパラメータを付加的にタイムスタンプの要求メッセージを含めるようにし、タイムスタンプサーバはこれらの情報を元にディジタル署名をしている。このため、どのようなアルゴリズムを用いてメッセージダイジェストを生成したか、証拠である返答メッセージに含まれているため、どのようにして証拠を検証すればいいのかがわかる。また、実際にデータのメッセージダイジェストを生成した方法とは別の方法で検証時にメッセージダイジェストを作成することが防げるので、偽証を防ぐことができる。

【００６１】また、データのメッセージダイジェストの代わりに暗号化したデータのメッセージダイジェストを署名対象データとすることで、タイムスタンプ生成時にはサーバに秘密にしておきたいデータに対してもタイムスタンプサーバに依頼することが可能となる。また、別の手段としてデータを暗号化して復号鍵のメッセージダイジェストを含め、復号鍵を公開鍵で暗号した時も同様の効果が得ることができる。

【００６２】また、データの作成者、電子メッセージの発信者や受信者の識別情報を暗号化して要求メッセージや返答メッセージを含めるようにしたので、タイムスタンプサーバやタイムスタンプサーバの運営者に知られることなくデータ作成者や電子メッセージの発信者・受信者を含めたデータの付加情報に対してタイムスタンプサーバの署名をもらうことが可能となる。

【図面の簡単な説明】

【図１】タイムスタンプサービスの全体構成、およびタイムスダンプサーバの内部構成図である。

【図２】メッセージダイジェストを含む要求メッセージ構成図である。

【図３】図２の要求メッセージに対する返答メッセージ構成図である。

【図４】暗号化したメッセージダイジェストを含む要求メッセージ構成図である。

【図５】図４の要求メッセージに対する返答メッセージ構成図である。

【図６】タイムスタンプサーバの基本動作を示すフローチャートである。

【図７】公開鍵証明書の有効性確認サービスと組み合わせた場合のタイムスタンプサーバの動作を示すフローチャートである。

【図８】タイムスタンプ証明書を用いたデータの存在を確認する証明者公証人の動作を示すフローチャートである。

【図９】請求項１で公開鍵を使った場合の要求メッセージ構成図である。

【図１０】請求項１で公開鍵を使った場合のデータの存在を確認する証明者公証人の動作を示すフローチャートである。

【符号の説明】

１１０…タイムスタンプサーバ、１１１…公開鍵証明書DB、１１２…ディジタル署名処理器、１１３…要求・返答メッセージ処理器、１１４…時計、１１５…通信器、１２０…ネットワーク、１３０…クライアント、１４０…タイムスタンプサービスシステム、２０１…タイムス

タンプ対象データのメッセージダイジェスト及び付加的にアルゴリズムとパラメータを暗号した結果、２０２…201を復号する鍵のメッセージダイジェスト、２０３…201の暗号に使用したアルゴリズムの識別子、２０４…201の暗号に使用したパラメータ、３０１…ディジタル署名の生成日時、３０２…証明対象データ、３０３…サーバの署名、３０４…署名生成アルゴリズム識別子、３０５…署名生成パラメータ、４０１…タイムスタンプ対象データのメッセージダイジェスト、４０２…メッセージダイジェストアルゴリズム識別子、４０３…メッセージダイジェストパラメータ、４０４…タイムスタンプ対象文書の形式、４０５…タイムスタンプ対象文書のタイトル、４０６…タイムスタンプ対象文書の作成者、４０７…有効性確認を行う公開鍵証明書の識別子、４０８…公開鍵証明書の有効性確認を行う日時、５０１…要求メッセージ受付日時、５０２…署名対象データ、５０３…公開鍵証明書有効性確認結果、５０４…公開鍵証明書無効理由、５０５…公開鍵証明書無効日時、５０６…公開鍵証明書シリアル番号、５０７…サーバの署名、９０１…暗号データ、９０２…暗号した復号鍵、９０３…公開鍵、９０４…公開鍵暗号アルゴリズム識別子、９０５…暗号データ暗号アルゴリズム識別子。

【手続補正２】

【補正対象書類名】図面

【補正対象項目名】図１

【補正方法】変更

【補正内容】

【図１】

図１